

REMARKS

In response to the Office Action mailed October 5, 2004, Applicants respectfully request reconsideration. Claims 1-66 were previously pending in this application. No claims have been amended, canceled or added by this request. As a result, claims 1-66 are pending for examination with claims 1, 23, 27, 32, 57 and 62 being independent claims. To further the prosecution of this application, each of the rejections set forth in the Office Action has been carefully considered and is addressed below. The claims as presented are believed to be in allowable condition.

I. Rejections Under 35 U.S.C. §102

Claims 1-66 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 6,343,324 (Hubis et al.). Applicants respectfully traverse this rejection.

A. Claims 1 and 32

The Office Action asserts that column 5, lines 45-57; column 12, lines 27-35; column 14, line 40 – column 15, line 52; and Figure 3b of Hubis disclose a method showing each of the limitations of claim 1 (and that claim 32 is substantially the same as claim 1 and is rejected for the same reasons). Applicants respectfully disagree.

The method described in the above excerpts from Hubis involves setting up permission tables to logical volumes of a storage device according to access rights associated with a host's World Wide Name (WWN) during a login procedure, and indexing the permission tables during subsequent read/write requests to the logical volumes (Columns 14, 15 and FIGS. 3A and 3B, respectively). However, Hubis does not address problems of an untrusted environment where hosts may potentially spoof their identities (e.g., spoof their WWN). In particular, Hubis is completely silent with respect to determining whether multiple accesses by a device representing itself as a particular device are made via the same physical connection, as discussed further below.

Hubis discloses a controller for handling access to a shared storage device from a plurality of host computers (Col. 4, lines 40-50). The access control method of Hubis can be generally separated into two distinct phases: 1) the login procedure illustrated in FIG. 3A; and 2) the request procedure illustrated in FIG. 3B. The login procedure adds entries into a number of tables that identify the host by its WWN and sets up permission tables that define the hosts

access profile (FIGS. 2B-1, 2B-2 and 2B-3). In particular, the login procedure establishes an entry in the Host WWN List 153 (FIG. 2B-1) which associates the host's WWN with a Host Index (HI), inserts an entry in the Host ID Map 155 (FIG. 2B-1) which associates the Host Index with the Fibre Channel Loop ID of the host, and sets a permission bit in a corresponding Volume Permission Table 194 (FIG. 2B-3) according to access rights indicated by WWN's stored in Volume Name Tables 130 (FIG. 2B-2), which are instantiated for each Logical volume of the shared storage device (Col. 14 line 40- Col. 15 line 9, and FIG. 3A).

A controller 106 manages the login procedure as follows. The controller 106 first determines that a host is attempting to login (Col. 14, line 45, FIG. 3A Step 302). The controller obtains the host's WWN 107 from the login information provided by the host and checks to see whether the WWN has been entered into the Host WWN List 155 (Col. 14, lines 45-47 and FIG. 3A, Step 305). If the WWN has been previously entered, the associated Host Index 151 is obtained from the Host WWN List (Col. 14, lines 48-50 and FIG. 3A, Step 306). If the WWN is not found, the WWN is added at the end of the Host WWN List and the Host Index for the host becomes the position of the new entry in the list (Col. 14, lines 50-53 and FIG. 3A, Step 307). The Host Index is then added into the Host ID Map 155 at the position indicated by the Fibre Channel Loop ID 152 of the host, both in circumstances where the WWN is found and in circumstances where the WWN is not found in the Host WWN List (Col. 14, lines 50-53 and FIG. 3A, Step 308).

The controller then collects information from the Fibre Channel I/O Processor at which the login attempt is being made to set a Permission Indicator 195 (or Permission Flag) corresponding to the host if it is determined that the host is authorized to access the requested volumes (Col. 14, lines 56 and 57). In particular, the controller 106 and I/O processor 184 at which the host is connected, and the Logical volume for which the login request is targeted, are used in combination to locate a corresponding Volume Permission Table 194 in the Port Mapping Table 190 (Col. 14, lines 56-66 and FIG. 3A, Step 312).

The Port Mapping Table (FIG. 2B-3) includes a Volume Permission Table for each combination of controller, I/O processor and Logical Volume (Col. 10, lines 47-51). Each Volume Permission Table is an array of one bit flags (Permission Indicator) that indicate whether the corresponding host is permitted to connect to the storage device (Col. 10, line 63 – Col. 11, line 7). The Volume Permission Table is indexed by the Host Index of the host. For example,

the Permission Indicator for the host with Host Index=5 will be the fifth bit in each Volume Permission Table (Column 15, lines 3-9).

The controller determines whether to set the Permission Indicator for a host to true (equal to 1) or false (equal to zero) by checking the Volume Name Table 130 (FIG. 2B-2) to verify that the WWN of the host has been granted access to the corresponding Logical volume (Col. 14, line 66 – Col. 15, line 3 and FIG. 3A, Step 313). Each Volume Name Table is associated with one of the Logical volumes available at the storage device and includes a list of WWN's that have permission to access the associated Logical volume (Col. 12, line 25-29). The controller searches the Volume Name Table of the Logical volume included in the login request, and if the WWN of the host is found in the table, the controller sets the Permission Indicator to 1, otherwise the controller sets the corresponding Permission Indicator to zero to complete the login procedure (Col. 15, lines 3-9 and FIG. 3A Steps 314 and 315).

In the request procedure, the controller processes an I/O command to read or write to a Logical volume as follows. When a request is received from a host, the controller locates the appropriate Port Mapping Table based on the controller and I/O processor at which the request was made, and the Logical volume targeted in the request (Col. 15, lines 19-27 and FIG. 3B, Steps 317-320). The Host Index for the host making the request is obtained by indexing the Host ID Map with the Loop ID (a portion of the Target ID provided in the command) of the requesting host (Col. 15, lines 27, 28 and FIG. 3B, Step 321). The Volume Permission Table is then examined at the position indicated by the Host Index to determine if the host was granted permission to access the Logical volume during the login procedure (Col. 15, lines 26-32 and FIG. 3B, Step 322).

It should be appreciated that at no time during either the login procedure or the request procedure does the controller determine whether a host representing itself as a specific host (e.g., via a WWN) is attempting to access the storage device over a same or different physical connection. In particular, the controller takes at face value all of the login information provided by the host. While the Volume Permission Table is organized according to the controller and I/O processor combination at which a host is attempting access, the controller does not check to ensure that this connection is consistent. A login attempt from a host at a different physical location will not result in denied access, but rather results in a new entry in the Volume Permission Table at the new controller/I/O processor combination. A simple example of a host

B attempting to spoof its WWN in the context of the above described login and request procedures will illustrate this point.

Assume that a host A has initially logged on using its authentic WWN and therefore has established entries in the tables described above (i.e., has established an entry in Host WWN List 153, Host ID Map 155 and set a Permission Indicator in the appropriate Volume Permission Table). When host B attempts to login using the WWN of host A, the controller will find the WWN in the Host WWN List 153 (i.e., at Step 307 in FIG. 3A) and the corresponding Host Index 151 will be obtained. The obtained Host Index is then inserted into the Host ID Map 155 at an entry corresponding to the Loop ID of host B. The controller does not check to see if the Loop ID of host B presently logging in is the same as the Loop ID already associated with the obtained Host Index (i.e., the Loop ID of host A). Rather, it generates a new entry associating the Loop ID of host B with the obtained Host Index. Column 14, lines 48-56 state:

If the WWN of the controller attempting the login is found (Step 306), the position of the host's WWN 107 in the Host WWN List 153 is the Host Index 151. If the WWN is not found, the WWN 107 of the host attempting the login is added to the end of the Host WWN List 153 (Step 307) and that position is the Host Index 151. The Host Index 151 is then placed into the Host ID Map 155 at the position indicated by the host's Fibre Channel Loop ID 152 (Step 308). (emphasis added).

It should be appreciated that the Host Index obtained from the Host WWN List will be added as an entry associated with the Loop ID of the host presently logging in regardless of whether a WWN entry is found or not (i.e., in FIG. 3A, step 308 is performed after either of steps 306 and 307). As such, host B will set up its own Host ID Map entry with its own Loop ID using host A's WWN. The controller will then set the Permission Indicator in the Volume Permission Table associated with the controller, I/O Processor and Logical volume combination of host B according to the access rights of host A's WWN (i.e., the spoofed WWN). Since the Permission Indicator is set exclusively by searching the Volume Name Table for the provided WWN and the spoofing host has set up an association between its own Loop ID and host A's Host Index, host B has successfully hijacked the volume access profile of host A.

When host B subsequently makes an I/O request, its real Loop ID will map to host A's Host Index (i.e., both hosts will have a Host ID Map entry containing their respective Loop IDs mapped to a shared Host Index). Since the login procedure established the access permissions of

host A in the Volume Permission Table associated with the location of host B (i.e., in Steps 309-313), the controller will accept any read/write command from host B that host A is permitted to make.

In Hubis, the controller takes the information provided by the host and establishes associations in the appropriate data structures without ever determining whether that information is authentic or consistent. For example, the Hubis reference nowhere discusses any mechanism for preventing multiple entries in the Host ID Map from being established, such as by a host using the same WWN from different physical locations on the network. Hubis simply lacks any disclosure relating to ensuring that hosts do not spoof their identity. In particular, Hubis is completely silent with respect to determining whether hosts that represent themselves with the same identity are attempting to access the storage device over different physical connections.

The Office Action asserts that column 15, lines 50-52 discloses a method of checking the physical connection, “where the access path qualifier is determined by the WWN ... and comparing it with the table entries.” (Office Action, Page 3). However, the WWN is a device specific identifier that is independent of the location of the device on the network. That is, the WWN indicates nothing about the physical connection of the device and, therefore, is insufficient to validate a physical connection. The controller of Hubis compares a presented WWN with current entries in the Host WWN List, but does so merely to ascertain whether the host has previously logged in, not to verify a physical connection as the WWN alone does not carry this information. In particular, the search of the Host WWN List simply determines whether a Host Index for the host already exists or whether one needs to be generated. However, this table search does not relate to, nor can it verify, the physical connection of the device.

Claim 1 recites a method for use in a computer system including a plurality of devices, a shared resource shared by the plurality of devices, and a network that couples the plurality of devices to the shared resource. The method includes acts of, in response to one of the plurality of devices attempting to access the shared resource and representing itself to the shared resource as a first device, determining whether the one of the plurality of devices is attempting to access the shared resource through a physical connection through the network that is different than a first physical connection through the network used by the first device to access the shared resource, and when it is determined that the one of the plurality of devices is attempting to access the shared resource through a connection through the network that is different than the first

physical connection, denying the attempted access by the one of the plurality of devices to the shared resource,

Nowhere does Hubis disclose or suggest “determining whether the one of the plurality of devices is attempting to access the shared resource through a physical connection through the network that is different than a first physical connection through the network used by the first device to access the shared resource,” as recited in claim 1. Therefore, claim 1 patentably distinguishes over Hubis and is in allowable condition.

Claims 2-22 depend from claim 1 and are allowable for at least the same reasons.

Claim 32 recites an apparatus for use in a computer system including a plurality of devices, a shared resource shared by the plurality of devices, and a network that couples the plurality of devices to the shared resource. The apparatus includes an input to be coupled to the network and at least one controller coupled to the input. Nowhere does Hubis disclose or suggest a controller to “determine whether the one of the plurality of devices is attempting to access the shared resource through a physical connection through the network that is different than a first physical connection through the network used by the first device to access the shared resource,” as recited in claim 32. Therefore, claim 32 patentably distinguishes over Hubis and is in allowable condition.

Claims 33-56 depend from claim 32 and are allowable for at least the same reasons.

B. Claims 23 and 57

The Office Action asserts that Hubis meets all of the limitations of claim 23 and that claim 57 is substantially similar to claim 23. Specifically, the Office Action asserts that column 9, lines 50-57 discloses “comparing a value of the second identifier presented by one of the plurality of devices to the stored value of the second identifier for the first device,” and column 10, lines 33-40 discloses “determining that the one of the plurality of devices is attempting to login to the storage system through a physical connection through the network that is different than the first physical connection when the value of the second identifier presented by the one of the plurality of devices mismatches the stored value of the second identifier for the first device.” Applicants respectfully disagree.

The disclosure at column 9, lines 50-57 merely states that the internally generated Host Index and the WWN are used to deny access to a host attempting to login. It should be appreciated that both the WWN and the Host Index are identifiers that are independent of the

connection topology of the network. In particular, the WWN is an identifier specific to a device, “usually in the form of a number (serial number) that the manufacturer registers with the appropriate standards committee through the process defined as a part of the Fibre Channel standards specification. It is unique to each fibre channel connect device manufactured.” (Column 6, lines 40-45). The Host Index is a number generated by the controller in association with the WWN such that “a particular host computer’s Host Index (HI) 151 *remains the same regardless of the port* or controller the host is communicating with (emphasis added).” (Column 9, lines 49-51). That is, both identifiers remain persistent regardless of where a host is located on the network and therefore is independent of the physical configuration of the computer system.

In claim 23, the second identifier is recited as uniquely identifying the device “in a manner that is *dependent* upon the physical configuration of the computer system.” (emphasis added). As discussed above, both the WWN and the Host Index are identifiers that are *independent* of the physical configuration and therefore are not “second identifiers” as recited in claim 23. Neither in the above excerpt pertaining to the Host Index and WWN, nor anywhere in Hubis does it disclose or suggest a method including an act of “comparing a value of the second identifier presented by one of the plurality of devices to the stored value of the second identifier for the first device,” wherein the second identifiers identify the device “in a manner that is dependent upon the physical configuration of the computer system,” as recited in claim 23. Therefore, claim 23 patentably distinguishes over Hubis and is in allowable condition.

In addition, not only does the type of information being compared distinguish over Hubis, but so does the purpose of the comparison. In the login procedure of Hubis, the only comparison that the controller makes relates to comparing the WWN provided by the host with WWN’s already entered into the Host WWN List to determine whether the host has already logged in. That is, Hubis compares two configuration independent identifiers to determine whether a host has already logged in or whether a new entry needs to be added. This is a different determination than that recited in claim 23. In particular, the comparison in Hubis is not a determination of where a host is logging in from. Hubis does not disclose or suggest comparing *any* type of information for the purpose of “determining that the one of the plurality of devices is attempting to login to the storage system through a physical connection through the network that is different than the first physical connection,” as recited in claim 23. Thus, claim 23 further distinguishes over Hubis.

Claims 24-26 depend from claim 23 and are patentable for at least the same reasons.

Claim 57 recites an apparatus for use in a computer system including a plurality of devices, a storage system shared by the plurality of devices, and a network that couples the plurality of devices to the storage system. The apparatus includes an input to be coupled to the network, a storage device and at least one controller coupled to the network and the storage device. Nowhere does Hubis disclose or suggest a controller to “compare a value of the second identifier presented by the one of the plurality of devices to the stored value of the second identifier for the first device,” nor does it compare any values to “determine that the one of the plurality of devices is attempting to access the storage system through a physical connection through the network that is different than a first physical connection used by the first device in logging into the storage system,” as recited in claim 57. Therefore, claim 57 patentably distinguishes over Hubis and is in allowable condition.

Claims 58-61 depend from claim 57 and are allowable for at least the same reasons.

C. Claim 27

The Office Action asserts that column 10, lines 33-40 disclose the limitation “in response to one of the plurality of devices attempting to login to the network and representing itself to the network as a first device, determining whether the one of the plurality of devices is attempting to login to the network through a port that is different than a first port of the network through which the first device previously logged into the network.” Applicant respectfully disagrees.

Column 10, lines 33-40 describe defining how Logical volumes are mapped via multiple controllers and I/O processors, and relates to the internal mapping of controller and I/O processor combinations to the storage volumes, not to which port a particular host is connected, nor whether such a connection is consistent. As Hubis discusses in the immediately following paragraph (i.e., column 10, lines 41-56), the logical volume mapping is implemented using the Port Mapping Table 191, which has an entry for each controller, I/O processor and Logical Volume combination. However, the Port Mapping Table 191 does not determine whether a device is attempting to login from a different port. As discussed above (and as detailed in column 14, line 27 – column 15, line 9, and FIG. 3A), during login, access permissions are solely described as being determined by whether the WWN provided in the login information is present in the Volume WWN Table for the targeted Logical volume. Nowhere in the above excerpt asserted in the Office Action, or in the entirety of the Hubis reference, does it disclose or suggest

“determining whether the one of the plurality of devices is attempting to login to the network through a port that is different than a first port of the network through which the first device previously logged into the network,” as recited in claim 27. Therefore, claim 27 patentably distinguishes over Hubis and is in allowable condition.

Claims 28-31 depend from claim 27 and are allowable for at least the same reasons.

D. Claim 62

The Office Action asserts that column 11, lines 45-57 and column 12, lines 4-35 disclose “at least one controller that is responsive to one of the plurality of devices attempting to login to the network and representing itself to the network as a first device, to determine whether the one of the plurality of devices is attempting to login to the network through a port that is different than a first port of the network through which the first device previously logged into the network, and to deny the attempted login by the one of the plurality of devices to the network when the one of the plurality of devices is attempting to login to the network through a port that is different than the first port.” Applicants respectfully disagree.

Column 11, lines 45-57 describe the use of the Volume WWN Table 130 to determine allowed and disallowed access to a specific logical volume, stating in relevant part: “if a host computer 101 sends a new command to controller 106, the controller validates the WWN, controller port, and LUN against data in the table 130 prior to servicing the host command.” It should be appreciated that Volume WWN Table 130 merely stores the WWN of hosts that are allowed to access each Logical Volume. The Volume WWN Table 130 does not store, nor can it verify, the port at which a device is attempting a login. Column 12, lines 4-35 goes on to explain in further detail that there exists a Volume WWN Table for each logical volume that contains a listing of each WWN that is permitted access such that each volume can be independently designated as accessible by any combination of hosts. This does not relate to determining whether a represented device is attempting to access storage through a different port.

Neither in the above excerpts, nor elsewhere does Hubis disclose or suggest “determining whether the one of the plurality of devices is attempting to login to the network through a port that is different than a first port of the network through which the first device previously logged into the network,” as recited in claim 62. Therefore, claim 62 patentably distinguishes over Hubis and is in allowable condition.

Claims 63-66 depend from claim 62 and are allowable for at least the same reasons.

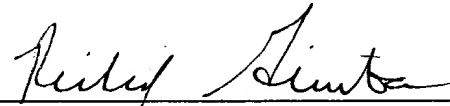
CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,
Steven M. Blumenau et al., Applicant(s)

By:


Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000

Docket No.: E0295.70155US00
Date: February 7, 2005
x02/07/05x